

Elitarna przestrzeń wymiany doświadczeń
dyrektorów bezpieczeństwa informacji



Modelowanie Zagrożeń

O krętej drodze na szczyt

Andrzej Dyjak
Filip Brandt

O MNIE

Rozwijam umiejętności zespołów i doradzam w zakresie najlepszych praktyk dla bezpiecznego procesu wytwórczego (SDLC).

- Bezpieczny Kod - Doradztwo i Szkolenia
    - Ofensywne Testowanie Web Aplikacji - kurs online
    - Automatyzacja Bezpieczeństw w Potoku CICD: DevSecOps - kurs online
- YouTube + Podcast







AGENDA

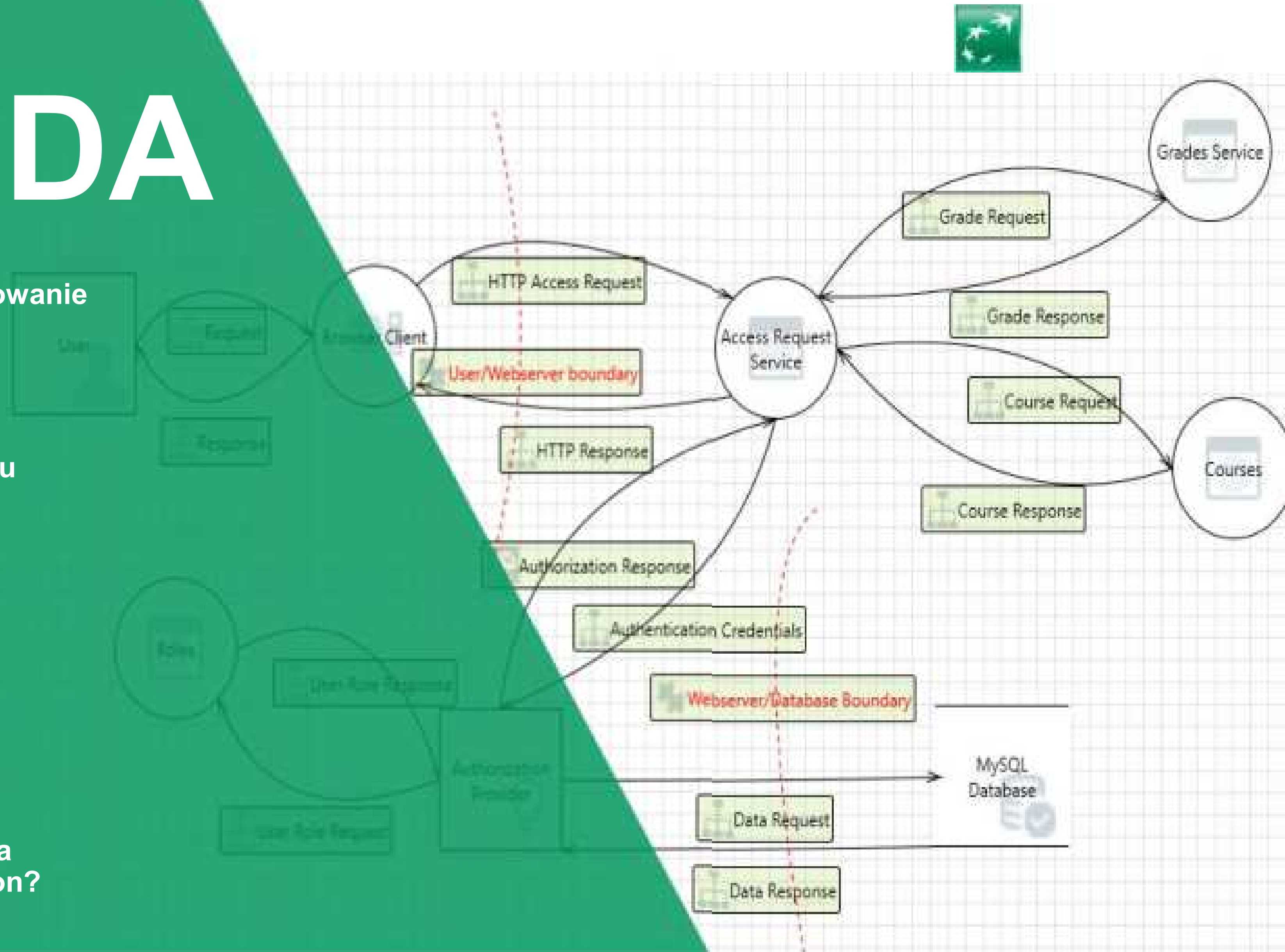
01 **Czym jest modelowanie zagrożeń?**

02 **Jakie mamy dostępne na rynku narzędzia?**

03 **Czy można to automatyzować?**

04 **Jak mierzyć skuteczność?**

05 **Jaką rolę odgrywa Security Champion?**



BNP PARIBAS

Modelowanie Zagrożeń

101

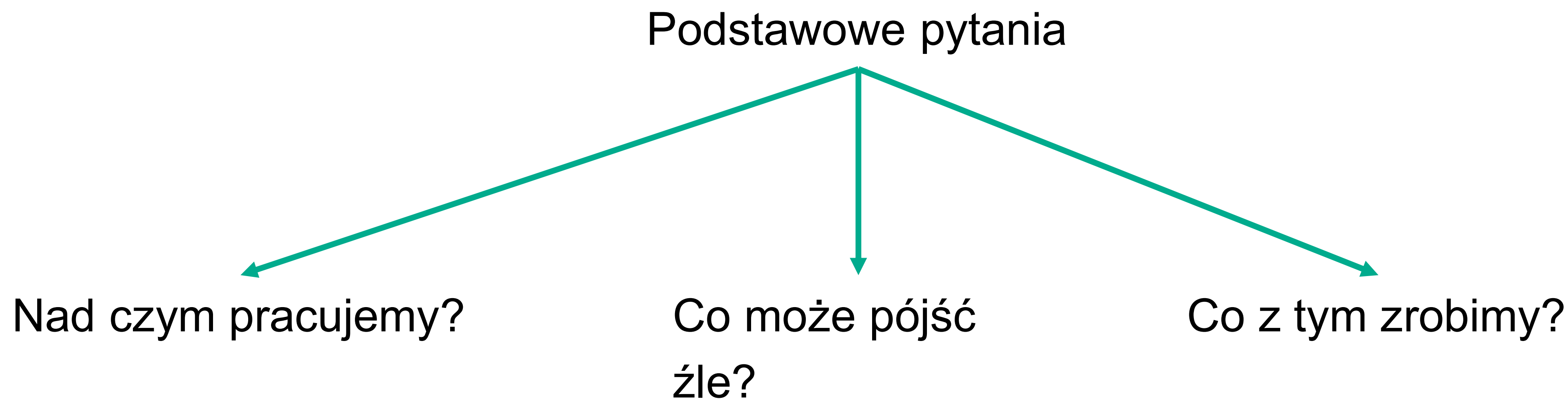
MODELOWANIE ZAGROŻEŃ - 101

Analiza reprezentacji systemu w celu podkreślenia problemów związanych z bezpieczeństwem lub prywatnością.

MODELOWANIE ZAGROŻEŃ - 101

Analiza **reprezentacji systemu** w celu podkreślenia problemów związanych z **bezpieczeństwem** lub **prywatnością**.

MODELOWANIE ZAGROŻEŃ - 101

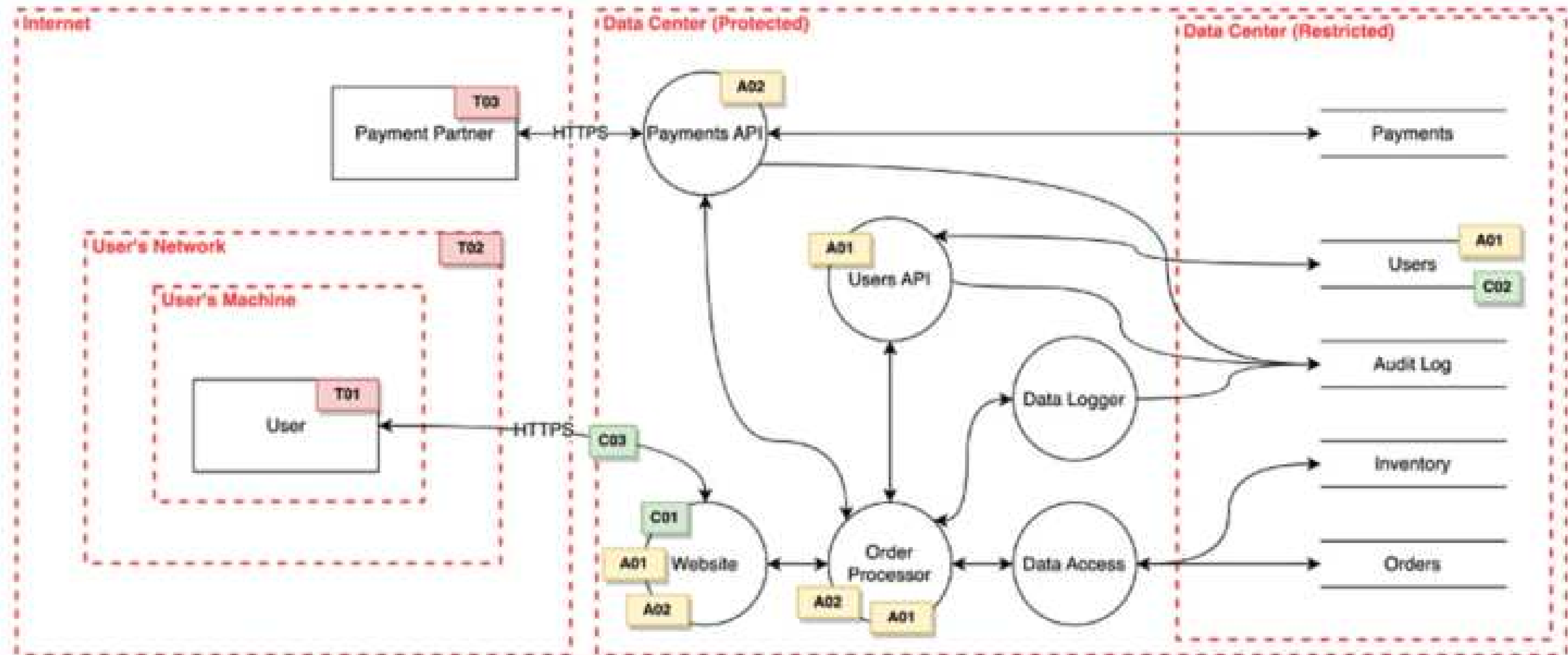


BNP PARIBAS

"**Proces** jest szerszy niż pojedyncza **sesja**"

BNP PARIBAS

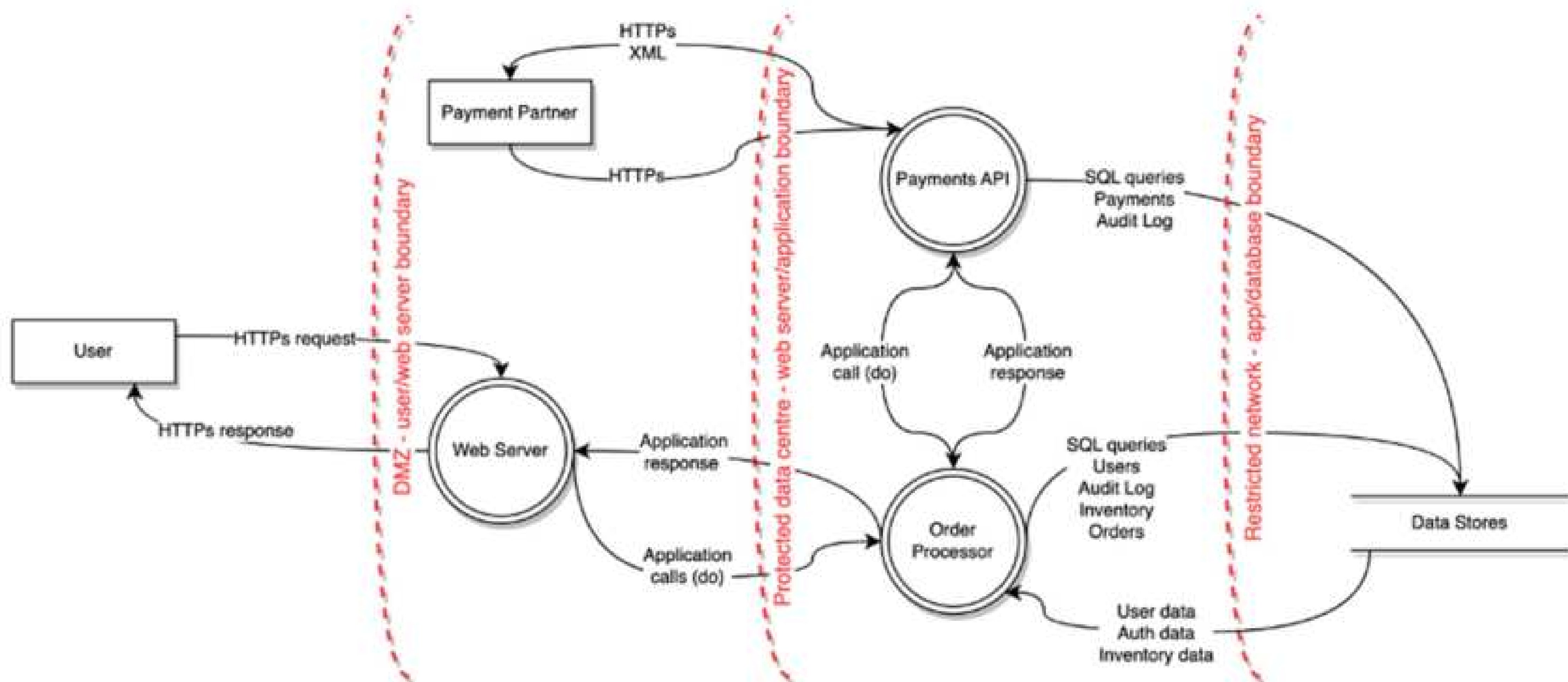
Poziomy Modelowania Zagrożeń



Assets	
ID	**Description**
A01	User Credentials
A02	Credit card data

Security Controls	
ID	**Description**
C01	Authentication
C02	Password hashing
C03	TLS

Threat Actors	
ID	**Description**
T01	Malicious user
T02	Man-in-the-middle
T03	Compromised payment partner


HTTPs
XML
Payment Partner
HTTPs
Payments API
SQL queries
Payments
Audit Log
User
HTTPs request
HTTPs response
DMZ - user/web server boundary
Protected data centre - web server/application boundary
Restricted network - app/database boundary
Application
call (do)
Application
response
Web Server
Application
response
Application
calls (do)
Order
Processor
SQL queries
Users
Audit Log
Inventory
Orders
Data Stores
User data
Auth data
Inventory data

MODELOWANIE ZAGROŻEŃ - 101

Różne punkty procesów SDLC

Różni ludzi (role)

Różne spojrzenia na system

MODELOWANIE ZAGROŻEŃ - 101

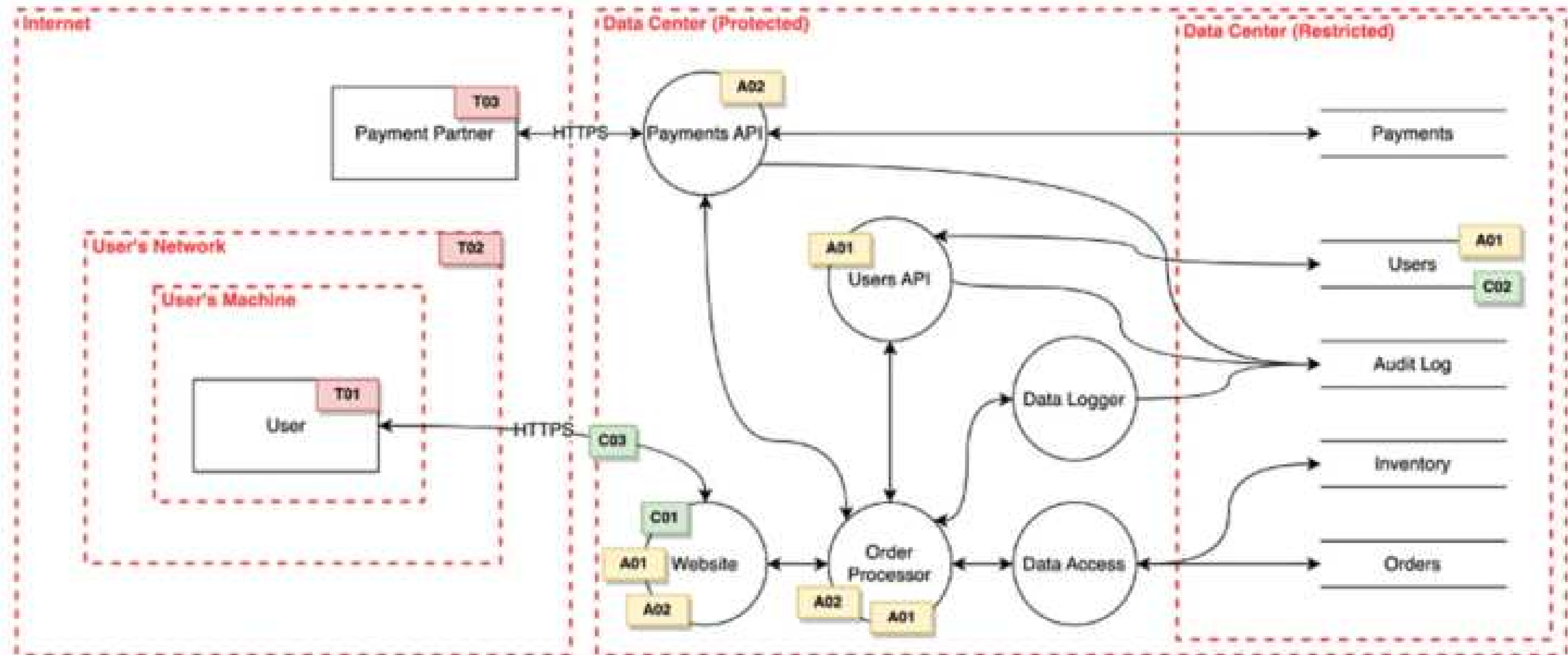
Różne punkty procesów SDLC

Różni ludzi (role)

Różne spojrzenia na system

Wyzwanie:
Co jest wyzwalaczem procesu? Kiedy powinien zaistnieć? Jak on wygląda? Kto ma modelować te zagrożenia?

Czy możemy używać tych samych narzędzi?



Assets

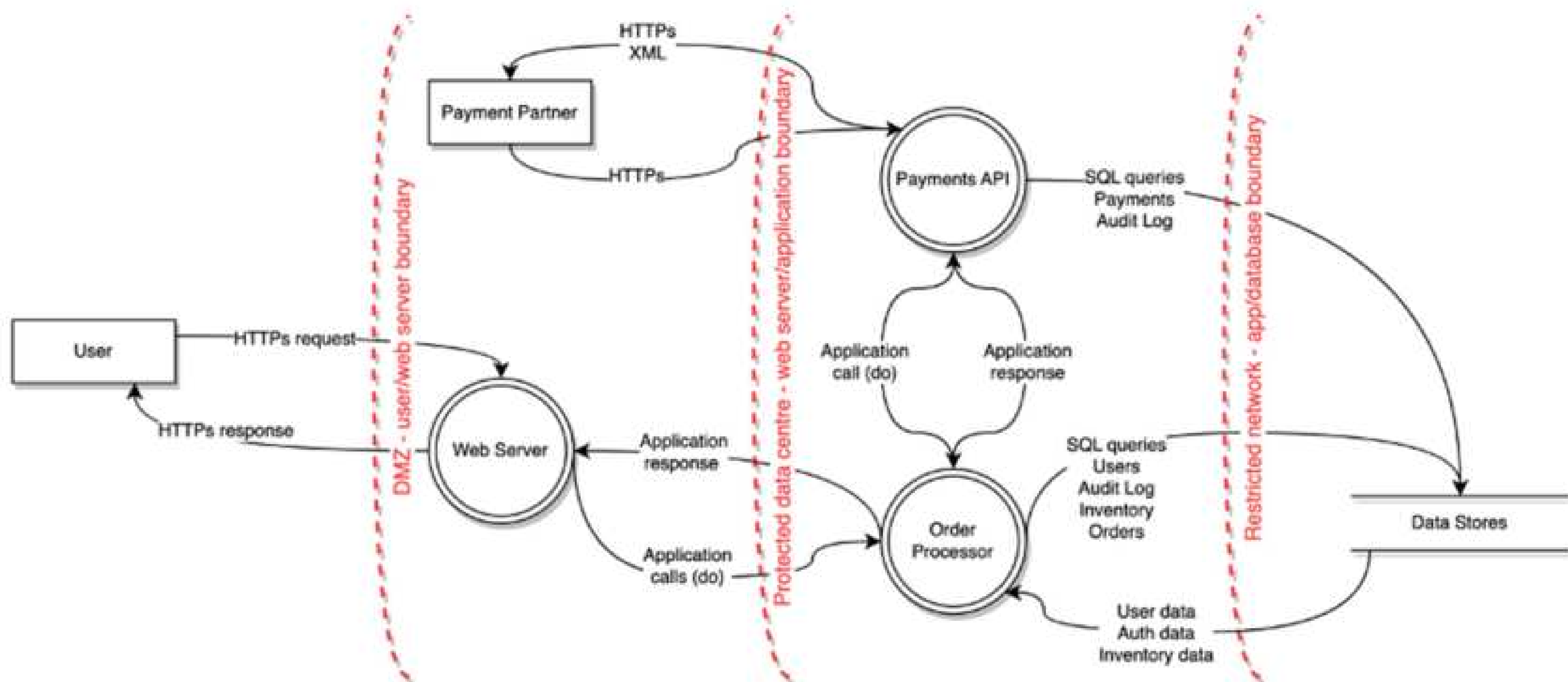
ID	Description
A01	User Credentials
A02	Credit card data

Security Controls

ID	Description
C01	Authentication
C02	Password hashing
C03	TLS

Threat Actors

ID	Description
T01	Malicious user
T02	Man-in-the-middle
T03	Compromised payment partner


HTTPs
XML
Payment Partner
HTTPs
Payments API
SQL queries
Payments
Audit Log
User
HTTPs request
HTTPs response
DMZ - user/web server boundary
Protected data centre - web server/application boundary
Restricted network - app/database boundary
Application
call (do)
Application
response
Web Server
Application
response
Application
calls (do)
Order
Processor
SQL queries
Users
Audit Log
Inventory
Orders
Data Stores
User data
Auth data
Inventory data

Proaktywność

vs Retroaktywność

BNP PARIBAS

NARZĘDZIA

Dostępne narzędzia

Procesowe

- **Metodyki** (Agile Threat Modelling, Rapid Threat Model Prototyping
- **Szukanie zagrożeń** (STRIDE, TRIM, OWASP TOP 10, CWE Top 25)
- **Priorytetyzacja** (DREAD, Risk Matrix)

Techniczne

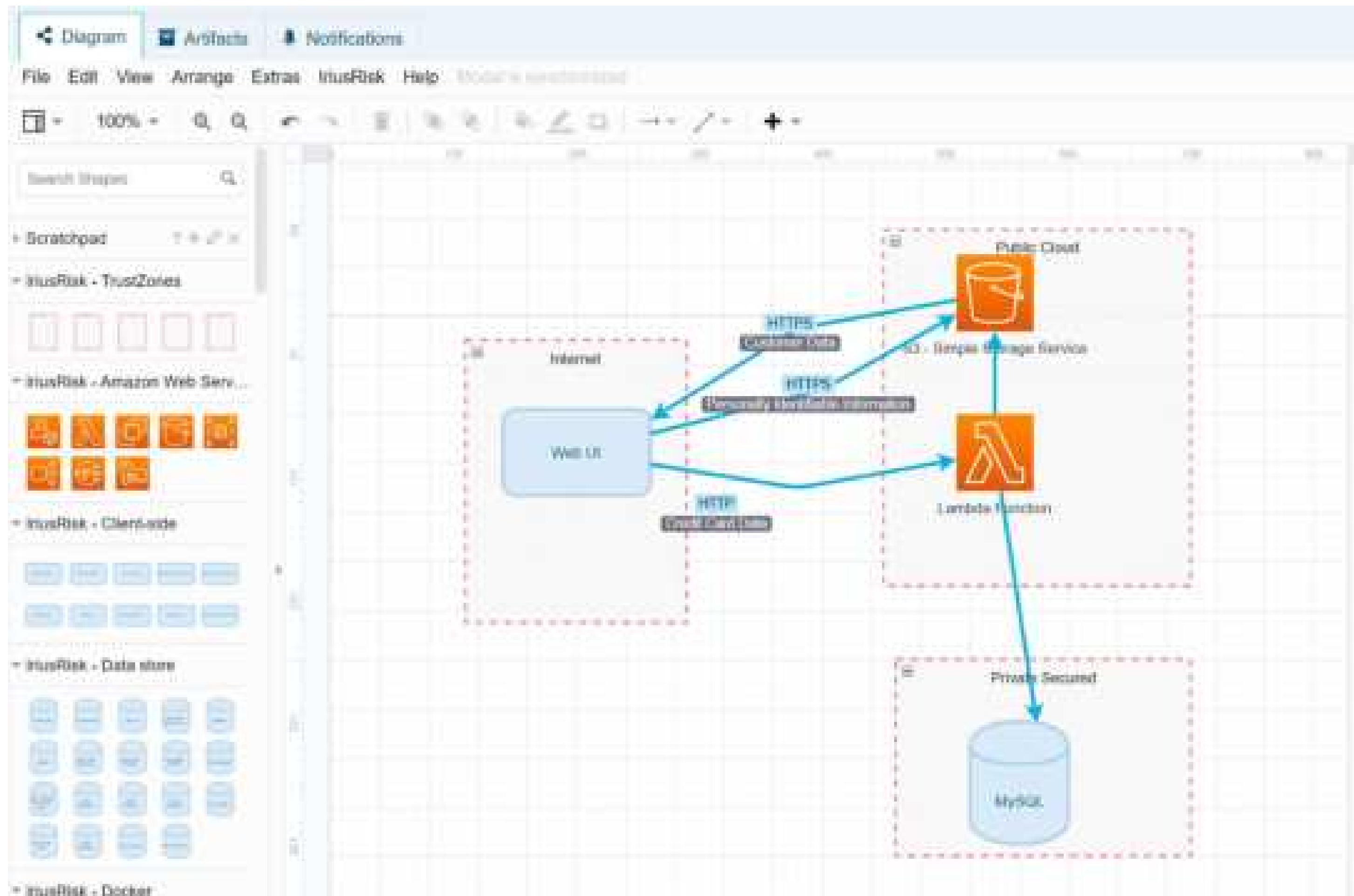
- **Darmowe**
  - Tablica
  - Microsoft Threat Modeling Tool
  - OWASP Threat Dragon
  - Draw.io
- **Komercyjne**
  - IriusRisk



Identity provider
User Profile
BFF
Customer service

https://www.iriusrisk.com/





A U T O M A T Y Z A C J A ?

Tak… Nie… To zależy ☺

MIARA SKUTECZNOŚCI

- Nie mierzyć bezpośredniego przełożenia na unikanie problemów (niewykonalne). Mierzyć za to ilościowo modele zagrożeń lub końcowe zagrożenia.
    - Dla podejścia **globalnego** lepiej mierzyć końcową ilość TM wraz z datą aktualizacji oraz pokrycie dla wybranych systemów.
    - Dla podejścia **iteracyjnego** lepiej mierzyć końcowe zagrożenia trafiające do backloga (i co się z nimi dzieje).

BNP PARIBAS

“

Hipotezę można
zwalidować
dopiero „po czasie“

”

Security Champions

BNP PARIBAS

SECURITY CHAMPION

- Must have, szczególnie w podejściu iteracyjnym. Czemu?
- Duże wyzwanie: Brak wiedzy i umiejętności.
- Dodatkowe korzyści:
  - Doskonalenie pętli zwrotnej.
  - Poczuwanie się do „ownershipu“ procesu.

JAK TO WYGLĄDA W BNP?

- Dwa potoki modelowania: Globalny (punktowe) i Iteracyjny (ciągłe, na poziomie sprintów).
- Główny driver to metodyka. W BNP poszliśmy w **Agile Threat Modeling (ATM)**.
- Narzędzie to **Draw.io** + dedykowany szablon **DFD/PFD** (wbudowany w narzędzie)
- Co pomaga myśleć o zagrożeniach?
  - **STRIDE** od strony bezpieczeństwa, **TRIM** od strony prywatności
  - **Top 10** i **ATT&CK** jako biblioteki ataków.
- Duże **wsparcie i entuzjazm** ze strony Security Championów.
- Automatyzacja? Na ten moment NIE, ale ATM pozwala przejść na RTMP, a z RTMP można myśleć o automatyzacji… więc jest na horyzoncie.

Dziękujemy!

https://dyjak.me

https://bezpiecznykod.pl

https://ofensywnetestowanie.pl

https://abcdevsecops.pl

